BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-268844
(43)Date of publication of application : 24.09.1992

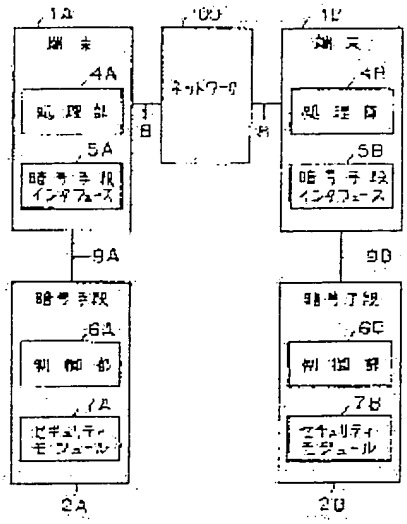
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G06F 15/00
G09C 1/00

(21)Application number : 03-028602
(22)Date of filing : 22.02.1991

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MIYAGUCHI SHOJI
MORITA HIKARI

(54) CIPHER USING METHOD AND MEANS THEREFOR

(57)Abstract:
PURPOSE: To make a ciphering method to be used differ for every user.
CONSTITUTION: When at a terminal 1A, a ciphering means 2A is given the instruction of a key sharing method, the ciphering means 2A ciphers a common key KS2 by an initial key KS1, and sends this cipher text C2 to the terminal 1A. The terminal 1A sends C2 to the terminal 1B, and the terminal 1B sends C2 to the ciphering means 2B. The ciphering means 2B decodes C2 by the initial key KS1, and obtains the common key KS2. In the terinals 1A and 1B, data is cipher-processed by the common key KS2 by each ciphering means 2A, 2B, and is sent to the terminal, and is sent to an opposite party. The ciphering means 2A, 2B can be exchanged to the terminals 1A, 1B, and another ciphering method can be used by exchanging the ciphering means. The terminal can not know what ciphering program is used.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－268844

(43)公開日　平成４年(1992)９月24日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
Ｇ０６Ｆ　15/00	３３０	Ｆ　7323－5Ｌ		
		7117－5Ｋ	Ｈ０４Ｌ　9／00	Ｚ

審査請求　未請求　請求項の数２(全　７　頁)　最終頁に続く

(21)出願番号　特願平3－28602

(22)出願日　平成３年(1991)２月22日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　宮口　庄司
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　森田　光
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

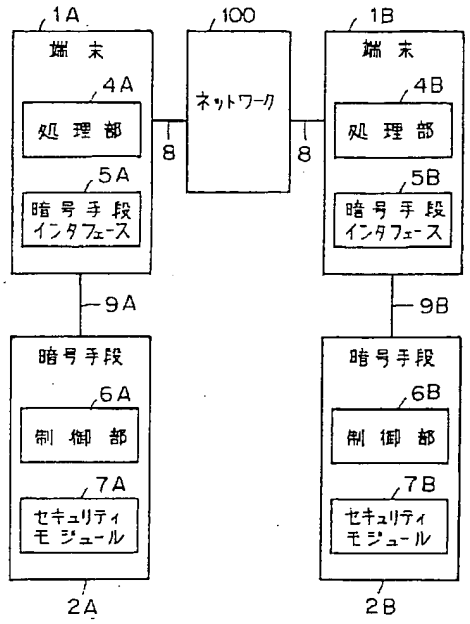
(54)【発明の名称】　暗号利用方法とその暗号手段

(57)【要約】

【目的】　利用者ごとに利用暗号方法を異ならすことを可能とする。

【構成】　端末１Ａで暗号手段２Ａに鍵共有方法を指示すると、暗号手段２Ａは初期鍵ＫＳ１で、共通鍵ＫＳ２を暗号化し、その暗号文C_2を端末１Ａへ送る。端末１ＡはC_2を端末１Ｂへ送り、端末１ＢはC_2を暗号手段２Ｂへ送る。暗号手段２ＢはC_2を初期鍵ＫＳ１で復号して共通鍵ＫＳ２を得る。端末１Ａ，１Ｂではそれぞれその暗号手段２Ａ，２Ｂでデータを共通鍵ＫＳ２で暗号処理し、端末へ送り、相手方へ送る。暗号手段２Ａ，２Ｂは端末１Ａ，１Ｂに対し交換可能であり、暗号手段を取替えて他の暗号方法を利用できる。端末はどのような暗号プログラムか知ることはできない。

図１



1

【特許請求の範囲】

【請求項１】　端末利用者が、端末間で暗号を利用する暗号利用方式において、それぞれの端末に暗号手段を取外し自在に結合し、それぞれの暗号手段は制御部とセキュリティモジュールとからなり、そのセキュリティモジュールは、端末利用者が予め個別に適宜決めて搭載してある一個以上の暗号処理機能を含み、端末は、データを暗合手段に転送して暗号処理し、その暗号処理されたデータを返却してもらうことを特徴とする暗号利用方法。

【請求項２】　請求項１の暗号利用方法において、上記暗号手段は、マイクロプロセッサと、暗号ＬＳＩ、暗号プログラムのいづれかの一個以上とを搭載するＩＣカードや光カードからなることを特徴とする暗号手段。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、ネットワークに加入した電話機、ファックス端末、テレックス端末、自動車電話機などの様々な端末が、秘密にするためにデータを暗号化して伝送するためや、データに対するディジタル署名をするためや、データが改ざんされているかの確認のために暗号を利用する方法に関する。

【０００２】

【従来の技術】従来の暗号利用方法を図３を参照して説明する。ネットワーク（通信網）１００にはこれに加入した電話機１０１、ファックス端末１０２、テレックス端末１０３、自動車電話機１０４、個人携帯電話機１０５、パーソナルコンピュータ１０６、電子計算機１０７、データ通信端末１０８などの端末が接続されている。これら端末は、互いに暗号通信したり、或は、暗号を応用した信頼性の高い通信、つまりディジタル著名、データ改ざん有無の確認など暗号を利用した通信を行なう。ネットワーク１００は、国内ネットワークや、国際ネットワークである。端末間で暗号通信を行うには、同じ暗号を使わなければならない。このためには、各端末が共通の暗号化および復号化手段をもつ必要がある。

【０００３】しかし次のような問題がある。即ち、①暗号はＩＳＯ等で国際標準化が行われていない、このため、国際的な規模で、各端末が共通に使える暗号が存在しない、②端末によっては暗号化手順が秘密の暗号を利用したい、③暗号が破れた場合は、直ちに他の暗号に切り替えたい、等の暗号利用上の問題や要求がある。従来の暗号利用上の問題や要求に答えられる暗号方式、即ち、ネットワークに加入した全ての端末が共通の暗号を使わなくともよく、暗号化手順が秘密の暗号を利用でき、更に、暗号の切り替えが容易に出来、しかも安全性が高い暗号の利用方法は提案されていなかった。

【０００４】この発明の目的は、ネットワークに加入した全ての端末が、共通の暗号を使わなくともよく、暗号化手順が秘密の暗号も、また、暗号化手順を公開した暗号も利用でき、暗号の切り替えが容易に出来、しかも安全性が高い暗号利用方法を提供することにある。この発明の説明に先立ち、暗号に関する用語を説明する。

2

（暗号化と復号化、暗号アルゴリズム）暗号化とは、平文ｐを、暗号化アルゴリズムＥにより、鍵ｋ１で暗号化し、暗号文ｃを得ることを言う。これを、数式で次のように表す。

ｃ＝Ｅ（ｋ１，ｐ）

復号化とは、暗号文ｃを、復号化アルゴリズムＤにより、鍵ｋ２で復号化し、平文ｐを得ることを言う。これを、数式で次のように表す。

ｐ＝Ｄ（ｋ２，ｃ）

ここで、暗号化アルゴリズムＥと復号化アルゴリズムＤは対になっており、両者を併せて、単に、暗号アルゴリズムという。

【０００５】ｋ１＝ｋ２であるとき、暗号アルゴリズムは、秘密鍵暗号アルゴリズム、または単に秘密鍵暗号という、ｋ１≠ｋ２であるとき、暗号アルゴリズムは、公開鍵暗号アルゴリズム、または単に、公開鍵暗号と呼ばれる。秘密鍵暗号では、ｋ１およびｋ２を秘密にする。公開鍵暗号では、ｋ１を公開する。但し、ｋ２は秘密とする。

（鍵の共有）端末ＴｉとＴｊとが、同じ暗号鍵を持つことを鍵の共有という。鍵の共有方法は様々なものがあり、次に４つの鍵共有の方法を説明する。これは、この発明の実施例において引用する。

【０００６】第１の鍵共有方法は、端末ＴｉとＴｊが、共有する鍵ＫＳ１を、予め端末内部のメモリに保持しておくことである。これは、例えば端末ＴｉやＴｊの所有者が、通信手段を使わずに、手操作で鍵ＫＳ１をその端末に設定することで達成される。共有する鍵が１個の場合もあれば、複数の場合もある。複数の場合は、鍵に番号や名前をつけておいて共有する鍵を区別する。鍵ＫＳ１を初期鍵という。

【０００７】第２の鍵共有方法は、秘密鍵暗号を用いて、セッション鍵ＫＳ２を端末ＴｉからＴｊへ配送する方法である。即ち、端末Ｔｉは、セッション鍵ＫＳ２を、初期鍵ＫＳ１で暗号化し、即ち、Ｃ２＝Ｅ（ＫＳ１，ＫＳ２）として、暗号文Ｃ２を得て、このＣ２を端末Ｔｊに送る。端末Ｔｊは、Ｃ２を復号化して、即ち、ＫＳ２＝Ｄ（ＫＳ１，Ｃ２）としてＫＳ２を得る。端末ＴｉとＴｊは、予め暗号化アルゴリズムＥと復号化アルゴリズムＤを決めておき、これら暗号アルゴリズムの実現手段を保持している。

【０００８】第２の鍵共有の詳細は、例えば国際標準ＩＳＯ８７３２に規定される。セッション鍵とは、通信セッションの都度変更する鍵を意味する。第３の鍵共有方法は、公開鍵暗号を用いて、セッション鍵ＫＳ３を端末ＴｉからＴｊへ配送する方法である。端末Ｔｉは、セッション鍵ＫＳ３を暗号化し、即ち、Ｃ３＝Ｅ（ＫＳ1_1，ＫＳ３）として、暗号文Ｃ３を得て、このＣ３を

3

端末Ｔｊに送る。端末Ｔｊは、Ｃ３を復号化して、即ち、ＫＳ３＝Ｄ（ＫＳ1_T，Ｃ３）としてセッション鍵ＫＳ３を得る。ここで、Ｅは公開鍵暗号の暗号化アルゴリズム、Ｄは公開鍵暗号の復号化アルゴリズムである。ＫＳ1_Iは公開鍵、ＫＳ1_Tは秘密鍵である。ここで示した鍵共有の詳細は、例えば、次の文献に解説される。

【０００９】W.Diffie and Hellmann 'New direction in cryptography',IEEE Transacti-ons. Information Theory, IT-22, 6, PP644-654, November 1976.第４の鍵共有方法は、端末ＴｉとＴｊの間でパラメータの変換値を変換し、セッション鍵ＫＳ４を計算する方法である。両者は鍵生成手段を持つ。これら鍵生成手段の機能を関数Ｆで表すと、

ＫＳ４＝Ｆ（Ｇ（ｐ１），ｐ２）

である。ここで、ｐ１とｐ２は、鍵生成手段に与えるパラメータであり、Ｇ（ｐ１）やＧ（ｐ２）は、パラメータの変換値である。関数ＦとＧは、Ｆ（Ｇ（ｐ１），ｐ２）＝Ｆ（Ｇ（ｐ２），ｐ１）となる性質を有する関数であり、更に、Ｇ（ｐ１）からｐ１の値を求めること、及び、Ｇ（ｐ２）からｐ２の値を求めることは、事実上不可能である。例えば、大型計算機を何千年間連続運転しても、ｐ１やｐ２を求められないという性質を有する。

【００１０】端末Ｔｉは、端末ＴｉのパラメータＲｉを決め、パラメータの変換値Ｇ（Ｒｉ）の値を端末Ｔｊへ送信し、端末Ｔｊは、端末ＴｊのパラメータＲｊを決め、パラメータの変換値Ｇ（Ｒｊ）の値を端末Ｔｉへ送信する。端末ＴｉとＴｊは、自己のパラメータと相手から送られてきたＧ（Ｒｊ）またはＧ（Ｒｉ）を用い、端末Ｔｉは、ＫＳ４＝Ｆ（Ｇ（Ｒｊ），Ｒｉ）の計算により、端末Ｔｊは、ＫＳ４＝Ｆ（Ｇ（Ｒｉ），Ｒｊ）の計算により、セッション鍵ＫＳ４を共有できる。パラメータを交換して鍵共有する方法は様々なものがあり、詳細は、例えば、文献、暗号と情報セキュリティの第４章（辻井重男編，昭晃堂，１９９０年）に、端末の名称（ＩＤ）を用いた鍵の共有方法として解説される。

（認証子の生成機能と認証子の確認機能）通信上のデータが改ざんされているか否かを検出するため、３２ビットの認証子を用いたデータ改ざんの検出機能は、データ改ざん検出関数G_{MAC}を用い、認証子の生成機能と認証子の確認機能により達成される。

【００１１】データ改ざん検出関数G_{MAC}は、鍵ＫＳと、長いデータＤＴとを入力し、３２ビット長の認証子（ＭＡＣ）を出力する。これを数式で書くと、

ＭＡＣ＝G_{MAC}（ＫＳ，ＤＴ）

認証子（ＭＡＣ）は、鍵ＫＳと、データＤＴとに依存して定まる性質を持つ特徴を持つ。関数G_{MAC}は、暗号化アルゴリズムを用いてつくられ、この暗号化アルゴリズムに入力する鍵が、データ改ざん検出関数G_{MAC}に入力する鍵であり、この暗号化アルゴリズムに入力する平文が、データ改ざん検出関数G_{MAC}に入力するデータである。データ改ざん検出関数G_{MAC}の具体的な作り方は、例えば、国際標準ＩＳＯ９７９７に規定される。

4

（データの改ざん検出）端末ＴｉとＴｊは、鍵ＫＳと、データ改ざん検出関数G_{MAC}の実現手段を持つ。端末Ｔｉが、データＸを、端末Ｔｊに送るとする。端末Ｔｉは、鍵ＫＳとデータＸを関数G_{MAC}に入力し、認証子ＭＡＣ１を生成する。即ち、ＭＡＣ１＝G_{MAC}（ＫＳ，Ｘ）とする。次に、端末Ｔｉは、データＸとＭＡＣ１とを通信回線を経由して、端末Ｔｊに送る。端末Ｔｊは、データＸとＭＡＣ１を受信し、自からも認証子を生成する。これをＭＡＣ２で表すと、ＭＡＣ２＝G_{MAC}（ＫＳ，Ｘ）となる。端末Ｔｊは、ＭＡＣ１とＭＡＣ２とが一致すれば、即ち、ＭＡＣ１＝ＭＡＣ２として、データＸが通信の途上で改ざんされなかったことが確認できる。データＸがＸ′に変化していると、即ち、Ｘ≠Ｘ′であるため、ＭＡＣ１≠ＭＡＣ２となり、データが通信途上で改ざんされたことが確認できる。

（データ圧縮機能）長いデータ、例えば６４×ｎビットや１２８×ｎビット長のデータを、６４ビットや１２８ビットにデータ圧縮する機能であり、ハッシュ関数ともいう。データ圧縮機能は、例えば国際規格ＩＳＯ１０１１８に規定される。

【００１２】その他特に説明しないが暗号を利用したディジタル著名もある。

【００１３】

【課題を解決するための手段】この発明によれば各端末に暗号手段が取外し自在に取付けられ、各暗号手段は制御部とセキュリティモジュールとからなり、制御部の機能は標準化しておき、セキュリティモジュールは、端末利用者が個別に必要とする暗号処理機能、例えば手順非公開の秘密暗号のプログラムや暗号ＬＳＩチップや、手順公開暗号のプログラムや暗号ＬＳＩチップ等を、予め個別に適宜決めて搭載してある。端末はデータを暗号手段に転送して暗号処理をしてもらい、その暗号処理済みのデータを返却してもらう。

【００１４】端末利用者毎に暗号手段の暗号方法を個別化することにより、暗号手段を交換して端末間で、様々な暗号の切り替えが容易に出来、しかも暗号処理は暗号手段で行われ、端末自体はどのような暗号が利用されているか不明であり、安全性が高い。

【００１５】

【実施例】図１にこの発明の実施例を示す。端末１Ａ，１Ｂはネットワーク１００に加入しており、この発明では端末１Ａ，１Ｂにそれぞれ暗号手段２Ａ，２Ｂが取外し自在に取付けられる。端末１Ａは処理部４Ａ、暗号手段インタフェース５Ａを備え、暗号手段２Ａは制御部６Ａ及びセキュリティモジュール７Ａを備えている。同様に、端末１Ｂは処理部４Ｂ、暗号手段インタフェース５

5

Ｂを備え、暗号手段２Ｂは制御部６Ｂ、セキュリティモジュール７Ｂを備えている。端末１Ａ，１Ｂは通信回線８でネットワーク１００に接続されている。端末１Ａ，１Ｂはそれぞれ暗号手段２Ａ，２Ｂと結合線９Ａ，９Ｂで結合されている。ここで、結合線９Ａは、端末１Ａと暗号手段２Ａ間でデータの流れがあること、また結合線９Ｂは、端末１Ｂと暗号手段２Ｂ間でデータの流れがあることを表す。暗号手段インタフェース５Ａや５Ｂ、及び、制御部６Ａや６Ｂの機能は、例えばＣＣＩＴやＩＳＯ等の国際的な範囲で標準化して用いる。

【００１６】処理部４Ａと４Ｂは、端末としての本来の機能を持つ。例えば、端末１Ａや１Ｂが電話機であるとき、処理部４Ａや４Ｂは電話機としての本来の機能を有し、端末１Ａや１Ｂがファックス端末であるときは、ファックス端末としての本来の機能を有し、端末１Ａや１Ｂがパソコンであるときは、パソコンとしての本来の機能を有す。端末１Ａと端末１Ｂは、通信回線８とネットワーク１００とを経由して通信する。暗号手段２Ａや２Ｂは、マイクロプロセッサと、暗号ＬＳＩや暗号プログラムのメモリチップのいづれかの一個以上とを搭載するＩＣカードや光カードなどの携帯が容易なものにより構成される。暗号手段インタフェース５Ａや５Ｂは、ＩＣカードあるいは光カードなどの暗号手段とのインタフェース処理部である。ここで光カードとは、光記憶部とマイクロプロセッサとを、１枚のカードに搭載したものを含む。制御部６Ａや６Ｂは、それぞれ、セキュリティモジュール７Ａや７Ｂが提供する機能を選択する機能と暗号手段インタフェース５Ａや５Ｂとのインタフェースを受持つ。セキュリティモジュール７Ａや７Ｂは、暗号処理機能、つまり暗号化、復号化機能、認証子の生成機能、認証子の確認機能、ディジタル署名機能、署名検証機能のいづれかの機能を少なくとも一以上実現する手段と、更に必要に応じて鍵共有機能、データ圧縮機能などを含む。制御部６Ａや６Ｂでは、例えば、選択番号１－１は、鍵共有方法１の機能を選択する、選択番号１－２は、鍵共有方法２の機能を選択する、・・・、選択番号２－１は、秘密鍵暗号Ｑの暗号化の機能を選択する、選択番号２－２は、ＦＥＡＬ暗号の暗号化機能を選択する、・・・、選択番号６はデータ圧縮機能を選択する、等と決めてあり、この決め方は例えば国内規格として標準化して使う。

【００１７】図２に、暗号手段２Ａのやや詳しい実施例を示す。セキュリティモジュール７Ａは、暗号化の実現手段、復号化の実現手段、認証子の生成実現手段、認証子の確認の実現手段のいづれかを１個以上複数含み、更に場合によると鍵共有手段やデータ圧縮手段などを含む。鍵共有の実現手段は、例えば、鍵共有の方法１や、鍵共有の方法２や、鍵共有の方法３や、鍵共有の方法４を行うためのプログラムを含み、更に、鍵共有のための補助機能、例えば乱数の生成機能などを含む。セキュリ

6

ティモジュール７Ａは、鍵共有方法１の初期鍵ＫＳ１を記憶している。初期鍵を複数保持する場合もあり、この場合は、複数の初期鍵を、番号あるいは名前により区別する。また、鍵共有方法２のセッション鍵ＫＳ２を記憶するメモリを含む。暗号化実現手段は、例えば、秘密暗号Ｑの暗号化プログラムやＤＥＳ暗号の暗号化プログラムであり、あるいは、暗号化モードで動作するＲＳＡ暗号のチップである。復号化実現手段は、例えば、秘密暗号Ｑの複合化プログラムやＤＥＳ暗号の復号化プログラムであり、あるいは、復号化モードで動作するＲＳＡ暗号のチップである。この場合、ＲＳＡチップは、ＩＣカードあるいは光カードに搭載されており、秘密暗号やＤＥＳ暗号のプログラムは、プロセッサに内蔵されたメモリに記憶されている。認証子の生成実現手段や認証子の確認の実現手段は、例えば、認証子生成プログラムや認証子の確認プログラムであり、プロセッサに内蔵されたメモリに記憶されている。ここで、秘密暗号Ｑとは、暗号手段２Ａや２Ｂを使う者が独自に定めた暗号化手順を公開しない暗号を意味する。データ圧縮手段は、例えば、国際規格ＩＳＯ１０１１８等で規定するデータ圧縮機能のプログラムであって、例えば、プロセッサに内蔵されたメモリに記憶されている。以上述べたセキュリティモジュール７Ａや７Ｂの暗号処理機能は、端末の利用者が予め個別に適宜決める。

【００１８】次に、この発明の暗号利用方法により、端末１Ａと端末１Ｂの間における、暗号通信や暗号を応用した通信方法を説明する。最初に端末１Ａが、第２の鍵共有の方法で端末１Ｂとセッション鍵ＫＳ２を共有後、平文データＸを秘匿して、端末１Ｂに送る例を説明する。端末１Ａの処理部４Ａは、暗号手段インタフェース部５Ａを経て、制御部６Ａに、第２の鍵共有方法により、端末１Ｂと鍵共有する機能を選択するように指示する。制御部６Ａは、セキュリティモジュール７Ａの内部にある第２の鍵共有方法を選択する。すると、セキュリティモジュール７Ａは、端末１Ｂと予め共有している初期鍵ＫＳ１を、セキュリティモジュール７Ａの記憶部から取り出し、次に乱数Ｒを生成する。セキュリティモジュール７Ａは、乱数Ｒを、端末１Ａと端末１Ｂ間の暗号通信用のための共有鍵ＫＳ２と定め（以降、セッション鍵ＫＳ２という）、即ち、ＫＳ２＝Ｒとし、このＫＳ２を、セキュリティモジュール７Ａの内部に記憶しておく。次に、このセッション鍵ＫＳ２を、初期鍵ＫＳ１で暗号化し、即ち、Ｃ２＝Ｅ（ＫＳ１，ＫＳ２）として、セッション鍵ＫＳ２の暗号文Ｃ２を得て、このＣ２を制御部６Ａを経て、更に、暗号手段インタフェース部５Ａを経て、処理部４Ａに送る。

【００１９】処理部４Ａは、暗号文Ｃ２を通信回線８を経て、端末１Ｂに送信する。端末１Ｂの処理部４Ｂは、暗号文Ｃ２を受信する。処理部４Ｂは、暗号手段インタフェース５Ｂを経て、制御部６Ｂに、第２の鍵共有方法

により鍵共有する機能を選択することの指示と共に、受信した暗号文Ｃ２を伝える。制御部６Ｂは、セキュリティモジュール７Ｂに対して、第２の鍵共有方法により鍵共有の選択指示と暗号文Ｃ２を伝える。すると、セキュリティモジュール７Ｂは、まず端末１Ａと共有している初期鍵ＫＳ１を、セキュリティモジュール７Ｂの記憶部から取り出し、次に暗号文Ｃ２を、鍵ＫＳ１で復号化し、即ち、ＫＳ２＝Ｄ（ＫＳ１，Ｃ２）として、セッション鍵ＫＳ２を得る。セキュリティモジュール７Ｂは、共有したセッション鍵ＫＳ２をその内部に記憶しておく。セキュリティモジュール７Ｂは、制御部６Ｂを経て、セッション鍵ＫＳ２を共有したことを、処理部４Ｂに知らせる。処理部４Ｂは、セッション鍵ＫＳ２を共有したことを、通信回線８を経て、端末１Ａの処理部４Ａに知らせる。以上で、端末１Ａと端末１Ｂ間で、セッション鍵ＫＳ２の共有を完了した。次に、端末１Ａの処理部４Ａが、平文データＸを暗号文に変えて、端末１Ｂの処理部４Ｂに伝える暗号通信を説明する。

【００２０】端末１Ａの処理部４Ａは、暗号手段インタフェース部５Ａを経て、制御部６Ａに、平文Ｘを暗号化する機能を選択するよう指示する。制御部６Ａは、処理部４Ａの指示に従い、平文Ｘをセキュリティモジュール７Ａに伝える。すると、セキュリティモジュール７Ａは、前記の方法で共有したセッション鍵ＫＳ２を、セキュリティモジュール７Ａの記憶部から取り出し、平文Ｘをセッション鍵ＫＳ２で暗号化し、即ち、Ｃ３＝Ｅ（ＫＳ２，Ｘ）として、暗号文Ｃ３を得て、このＣ３を制御部６Ａを経て、更に、暗号手段インタフェース部５Ａを経て、処理部４Ａに送る。処理部４Ａは、暗号文Ｃ３を、通信回線８を経て、端末１Ｂに送信する。端末１Ｂの処理部４Ｂは、暗号文Ｃ３を受信する。処理部４Ｂは、暗号手段インタフェース部５Ｂを経て、制御部６Ｂに、復号化の機能を選択する指示と共に、受信した暗号文Ｃ３を伝える。制御部６Ｂは、セキュリティモジュール７Ｂに対して、暗号文Ｃ３を復号化することを伝える。すると、セキュリティモジュール７Ｂは、前述した方法で共有したセッション鍵ＫＳ２を、セキュリティモジュール７Ｂの記憶部から取り出し、次に暗号文Ｃ３を、セッション鍵ＫＳ２で復号化し、即ち、Ｘ＝Ｄ（ＫＳ２，Ｃ３）として、暗号文Ｃ３を復号化して平文Ｘを得る。セキュリティモジュール７Ｂは、制御部６Ｂを経て、復号化して得た平文Ｘを、処理部４Ｂに知らせる。

【００２１】以上の説明は、鍵共有と暗号化および復号化が選択された例である。上記の説明において、セッション鍵ＫＳ２を共有後、処理部４Ａが、認証子の生成機能を指示する場合は、セキュリティモジュール７Ａの認証子生成手段が選択され、平文Ｘに対して、認証子ＭＡＣ１を生成し、即ち、$MAC1=G_{MAC}$（ＫＳ２，Ｘ）とし、平文ＸとＭＡＣ１とが、端末１Ａから、端末１Ｂに送られる。次に、端末１Ｂの認証子の確認手段が選択され、認証子ＭＡＣ１が正しいか否かが調べられる。

【００２２】この暗号利用方法を利用する者Ａ（Ｂ）は、自己の暗号手段２Ａ（２Ｂ）を携帯し、そのセキュリティモジュール７Ａ（７Ｂ）の内部に、例えば、秘密暗号Q_{AB}のプログラムと、ＲＳＡ暗号のプログラムとを組み込む。更に、この暗号利用方法の利用者Ａは、自己の他の暗号手段２Ａ′を持ち、そのセキュリティモジュール７Ａ′の内部に、自己が必要とする手段、例えば、秘密暗号Q_{AI}のプログラムを組み込む。この暗号利用方法の他の利用者B_Iは、自己の暗号手段２Ｂ′を持ち、その内部に秘密暗号Q_{AI}のプログラムを組み込む。ここで、秘密暗号Q_{AB}は、利用者ＡとＢの間で使う秘密暗号であり、秘密暗号Q_{AI}は、利用者ＡとB_Iの間で使う秘密暗号である。このようにすると、利用者Ａと利用者Ｂは、秘密暗号Q_{AB}とＲＳＡ暗号を内蔵する暗号手段を使って暗号通信が出来、また、利用者Ａと利用者B_Iは、秘密暗号Q_{AI}を内蔵する暗号手段を使って暗号通信が出来る。ここで、ＲＳＡ暗号は、暗号化アルゴリズムと復号化アルゴリズムが公開された、即ち、暗号化手順が公開された暗号である。

【００２３】以上述べたように、ネットワークに加入する端末の利用者は、それぞれ、自己が必要とする暗号の機能（例えば、鍵共有の機能、暗号化の機能、復号化の機能認証子の生成機能、認証子の確認機能、データ圧縮機能で、その機能は利用者が規定出来る）を内蔵した、いわば利用者毎に個別化された暗号手段２Ａ（２Ｂ）を持つ。また、暗号手段インタフェース５Ａや５Ｂは標準化してあるので、利用者毎に個別化された暗号手段２Ａや２Ｂは、どの端末１Ａや１Ｂとでも、結合して用いることが出来る。暗号の切り替えは、個別化された暗号手段を交換することにより達成できる。

【００２４】

【発明の効果】以上の実施例から明らかなように、この発明によれば暗号の利用者は、自己の用途のために個別化された暗号手段を用いることにより、自己が必要とする暗号の利用が可能である。この理由から、ネットワークに加入した全ての端末が、共通の暗号を使わなくともよく、暗号化手順が秘密の暗号も、また、暗号化手順を公開した暗号も利用でき、暗号の切り替えが容易に出来る暗号の使い方が可能である。しかも暗号処理は各暗号手段で行われ、これを端末で知ることができないから、高い安全性が得られる。

【図面の簡単な説明】

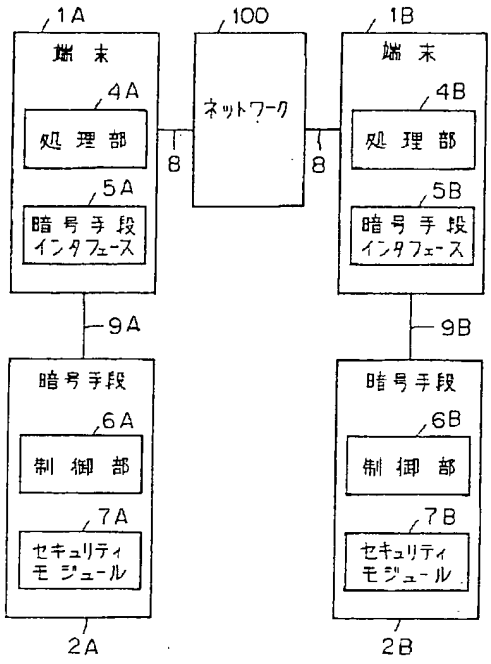
【図１】この発明の実施例を示すブロック図。

【図２】暗号手段２Ａの具体例を示すブロック図。

【図３】ネットワークを介した端末間通信の一般的構成を示すブロック図。

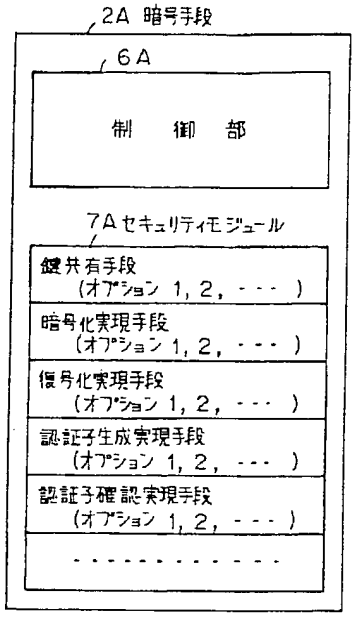
【図1】

図 1



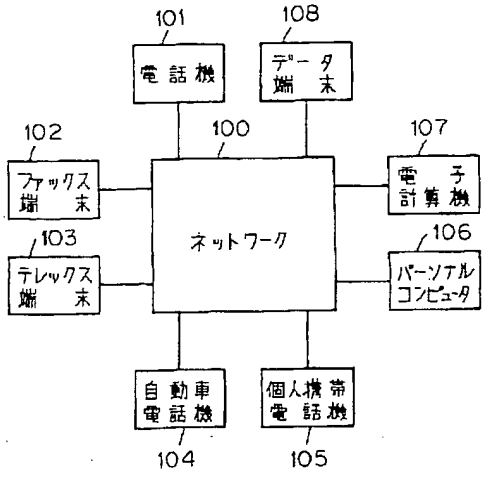
【図2】

図 2



【図3】

図 3



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
G09C 1/00		7922－5L		

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.